REMARKS

In the Office Action, claims 1-22 were rejected were rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent 6,182,216 (Luyster) in view of U.S. Patent 5,317,639 (Mittenthal).

By this Amendment, claims 3 and 5-6 are canceled. Thus, claims 1-2, 4 and 7-22 are pending. For at least the reasons set forth hereinbelow, Applicants request that the § 103(a) rejections associated with the pending claims be withdrawn.

Claims 1-2, 4 and 7-15

Applicant submits that independent claim 1 is nonobvious over the combination of Luyster and Mittenthal because the cited references fail to teach or suggest each and every element of claim 1. *See* MPEP § 2143 (stating that one of the elements of a *prima facie* case of obviousness under § 103(a) is that the prior art references, either alone or in combination, must teach or suggest every limitation of the claimed invention). More particularly, Applicant submits that the cited references fail to teach or suggest a method that includes, among other things, **deterministically** generating maximal nonlinear block substitution tables for a predetermined block size by "creating **maximal** nonlinear block substitution tables by combining the linear orthomorphisms" as recited in claim 1.

As disclosed in the specification, block substitution tables, also known as S-boxes, may be used in various cryptographic systems and methods. Although cryptographic block encryption can be accomplished in many ways, the block encryption process generally follows a well-known format. A block of clear text data, usually in the form of binary bits, is first broken down into sub-blocks of a given size (e.g., eight bits). The sub-blocks of clear text data then serve as the inputs to substitution tables. The outputs of the substitution tables are partially encrypted sub-blocks of the

same given size and are different than the inputs to the substitution tables. The partially encrypted sub-blocks then go through a permutation or inter-round mixing process that can involve bit or sub-block permutations, rotations, mixing with key or data bits, etc. This process may be repeated any number of times. For example, after the permutation or inter-round mixing process is completed, the resulting data may again be divided into sub-blocks that serve as inputs to substitution tables, and the resulting outputs of the substitution tables may then again go through the permutation or inter-round mixing process.

Whereas claim 1 recites a method of **deterministically** generating **maximal** non-linear block substitution tables for a predetermined block size, Applicant submits that Luyster merely teaches or suggests information relating to the inter-round mixing process. Thus, although Applicant respectfully disagrees with many of the Examiner's determinations concerning the teachings of Luyster, Applicant agrees with the Examiner's determination that Luyster fails to teach or suggest creating **maximal** non-linear block substitution tables as recited in claim 1. Applicant further submits that Luyster also fails to teach or suggest **deterministically** generating any kind of block substitution tables, let alone the type recited in claim 1.

Applicant also respectfully disagrees with the Examiner's determination that Mittenthal (the '639 patent) discloses using nonlinear orthomorphisms to create **maximal** nonlinear block substitution tables. Although Mittenthal (the '639 patent) discloses using linear orthomorphisms to create nonlinear orthomorphisms for block substitution tables, Applicant submits that Mittenthal (the '639 patent) is **silent** as to **deterministically** generating **maximal** nonlinear block substitution tables as recited in claim 1.

Applicant respectfully notes that when the '639 patent was filed, there were no known

methods of **deterministically** generating **maximal** nonlinear substitution tables. The absence of any known methods and the lack of **maximal** nonlinearity of the block substitution tables disclosed by Mittenthal (the '639 patent) prompted the additional research that eventually led to the invention recited in claim 1. Applicant also notes that unlike the maximal non-linear block substitution tables recited in claim 1, the nonlinear orthomorphisms taught by Mittenthal (the '639 patent) possess the property of lack of mutual information.

Thus, Applicant respectfully submits that it would not have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Luyster and Mittenthal (the '639 patent) to produce the invention recited in claim 1.

Therefore, for at least the reasons stated hereinabove, Applicant submits that claim 1 is nonobvious over the combination of Luyster and Mittenthal (the '639 patent) because the cited references fail to teach or suggest each and every element of claim 1. *See* MPEP § 2143 *id.* Applicant further submits that claims 1-2, 4 and 7-15, which depend from claim 1, are also nonobvious over the combination of Luyster and Mittenthal (the '639 patent). *See* MPEP § 2143.03 (stating that if an independent claim is nonobvious under §103(a), then any claim depending therefrom is nonobvious). Accordingly, Applicant respectfully requests that the §103(a) rejections associated with claims 1-2, 4 and 7-15 be withdrawn.

Claims 16-17

Applicant submits that independent claim 16 is nonobvious over the combination of Luyster and Mittenthal because the cited references fail to teach or suggest each and every element of claim 16. *See* MPEP § 2143 *id.* More particularly, Applicant submits that the cited references fail to teach

or suggest, among other things, "setting the maximal nonlinear block substitution tables based on a combination of the linear orthomorphisms, the substitution tables for use in encrypting clear text messages which are in the form of a sequence of binary numbers" as recited in claim 16.

For at least reasons similar to those set forth hereinabove with respect to claim 1, Applicant submits that claim 16 is nonobvious over the cited references. *See* MPEP § 2143 *id.* Applicant further submits that claim17, which depends from claim 16, is also nonobvious over the cited references. *See* MPEP § 2143.03 *id.* Accordingly, Applicant respectfully requests that the §103(a) rejections associated with claims 16 and 17 be withdrawn.

Claims 18-19

Applicant submits that independent claim 18 is nonobvious over the combination of Luyster and Mittenthal because the cited references fail to teach or suggest each and every element of claim 18. *See* MPEP § 2143 *id.* More particularly, Applicant submits that the cited references fail to teach or suggest, among other things, "setting the maximal nonlinear block substitution tables by combining the linear orthomorphisms, the substitution tables for use in encrypting clear text messages which are in the form of an ordering of binary numbers" as recited in claim 18.

For at least reasons similar to those set forth hereinabove with respect to claim 1, Applicant submits that claim 18 is nonobvious over the cited references. *See* MPEP § 2143 *id.* Applicant further submits that claim19, which depends from claim 18, is also nonobvious over the cited references. *See* MPEP § 2143.03 *id.* Accordingly, Applicant respectfully requests that the §103(a) rejections associated with claims 18 and 19 be withdrawn.

Claims 20, 21 and 22

For at least reasons similar to those set forth hereinabove with respect to claim 1, Applicant submits that independent claims 20, 21 and 22 are nonobvious over the combination of Luyster and Mittenthal (the '639 patent) because the cited references fail to teach or suggest each and every element of these claims. *See* MPEP § 2143 *id.* Accordingly, Applicant respectfully requests that the §103(a) rejections associated with claims 20, 21 and 22 be withdrawn.

CONCLUSION

Applicants respectfully request a Notice Of Allowance for the pending claims in the present application. If the Examiner is of the opinion that the present application is in condition for disposition other than allowance, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below in order that the Examiner's concerns may be expeditiously addressed.

Respectfully submitted,

Date: August 4, 2004

Robert A. Muha
Reg. No. 44,249

KIRKPATRICK & LOCKHART, LLP
Henry W. Oliver Building
535 Smithfield Street
Pittsburgh, Pennsylvania 15222

Telephone: (412) 355-8244
Facsimile: (412) 355-6501
E-mail: rmuha@kl.com